5250-3, Vol. V

Photovoltaics Program

Technology Development and Applications
Lead Center

Photovoltaic System Criteria Documents

Volume V: Safety Criteria for Photovoltaic Applications

10-15-79

Prepared for

U.S. Department of Energy

Through an agreement with
National Aeronautics and Space Administration

by

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

CONTENTS

SECTION I

SAFETY CRITERIA

A. SCOPE

This publication describes methodology for determining potential safety hazards involved in the construction and operation of photovoltaic power systems and provides guidelines for the implementation of safety considerations in the specification, design and operation of photovoltaic systems.

B. PURPOSE

This document will aid in the establishment of safety verification procedures for use in solar photovoltaic systems.

1. Reference documents

- "Performance Assurance Procedures Handbook, System Safety," Office of Fossil Energy Programs, DOE, (draft) March 1979.
- "Safety Procedures for the 25 kW Solar Photovoltaic Array at Mead, Nebraska," MIT/LL, April 1978.
- "Solar Photovoltaic Seminar, Part III, Special Safety Considerations," PRC Energy Analysis Co., (draft) June 1979.

C. SAFETY PROGRAM

The contractor is responsible for establishing a safety program in conformance with all applicable regulations, codes, standards and specifications. This program should be designed to use any existing effective procedures and practices which satisfy these guidelines. However, the specific methods of uncovering potential safety hazards mentioned herein must be considered and the generation of Hazards Analyses, Failure Mode and Effects Analyses, and Safety Audits are responsibilities of the contractor. The methods of performing these HA, FMEA and SA functions described in this document, however, are advisory, and equivalent methods are acceptable.

D. SAFETY PROGRAM PLAN

1. Failure Mode and Effects Analysis

The contractor shall perform a Failure Mode and Effects Analysis on the initial system design. This analysis will allow consideration of safety hazards both in the designed configuration and in perceived failure mode configurations. An example of an FMEA system is given in Appendix A. The FMEA will be updated and presented at the Critical Design Review.

2. Hazards Analysis

The contractor shall perform a preliminary Hazards Analysis early in the conceptual phase of the project so that safety considerations are included in tradeoff studies design alternative decisions. Subsystem and system Hazards Analyses shall be performed to identify hazards within the functions of the subsystems and the system as a whole. The effects on safety engendered by the failure modes determined by the FMEA shall be identified. An example of a Hazards Analysis is given in Appendix B.

3. Safety Audit

The contractor shall perform a System Safety Audit on the preliminary design. This audit will include both design configuration and system failure mode configurations as determined by the FMEA. The Safety Audit will be updated at the Critical Design Review and a final Safety Audit will be accomplished as a part of the final system Readiness Review. An example of a Safety Audit is given in Appendix C.

4. Safety Manuals and Admonitions

The contractor shall prepare safety manuals and admonitions as required to ensure safety in the construction and operation of the facility.

5. Safety Considerations in Design

The design of the facility will be accomplished with system safety in mind. The output of the FMEA, Hazards Analyses and Safety Audits will be fed back into the design process to minimize the hazards disclosed by the audits.

E. CRITERIA

The requirement for the contractor to perform a Hazards Analysis, FMEA, and Safety Audit on new contracts will normally be an inherent part of the contractor's System Safety Program Plan, provided in response to photovoltaics contract requirements.

Existing contracts may be modified to require submittal of a Systems Safety Program Plan incorporating the requirement to provide a Failure Mode and Effects Analysis, a Hazards Analysis, and a Safety Audit at the discretion of the DOE project manager. This decision will be influenced by the size, complexity, and amount of work remaining on the project being considered and also by the benefit that will be obtained.

F. SAFETY DATA

Lists of the actual and potential safety hazards uncovered during the design and operation of a solar photovoltaic project shall be submitted to the DOE Photovoltaics Lead Center. This information is to be incorporated in a reference document for use as an aid in the safety evaluation of future projects. An example of such a list is given in Appendix D.

4

APPENDIX A

FAILURE MODE AND EFFECTS ANALYSIS

A. INTRODUCTION

1. General

This "Procedure for Performing Failure Mode and Effects Analysis (FMEA)" is provided by DOE's Photovoltaics T&A Lead Center as a guide to aid contractors in performing the FMEAs that may be required by DOE photovoltaics contracts, and as an informative document for field center project managers. It is not intended to impose this document as a contract requirement, but rather to provide a systematic and uniform method to perform an FMEA.

The purpose of an FMEA, as addressed, is to provide an orderly, critical examination of potential failure modes of plants and equipment, and the causes of the failure modes, in order to assess the safety of various systems or components, to analyze the effect of each failure mode on system operation, and to identify the corrective action, i.e., design modifications. To be effective, the FMEA reporting must be thorough and accurate, and produce results that can be easily interpreted by management, engineering and technical personnel. This procedure defines the overall concept of an FMEA; what an FMEA is; and when an FMEA is required; it then provides a method for the performance, evaluation, and documentation of an FMEA.

B. APPLICATION

The objective of the Tests and Applications (T&A) subprogram is to obtain operational experience with complete photovoltaic systems in a range of applications. The main thrust of the T&A subprogram will be directed toward a carefully selected series of experiments in remote, residential, intermediate load center, and central station applications. In the latter three experimental areas, interaction with electric utility generation-transmission-distribution grids will be emphasized. The implementation of safety criteria is required in the planning and conduct of these experiments.

1. Failure Mode and Effects Analysis (FMEA)

FMEA, as considered in this procedure, is an orderly analytical procedure that will aid in the identification of potential weaknesses and hazards, and focus on the need for engineers to design effective, reliable and safe plants or equipment by:

- Identification of potential failures and failure modes
- Assessment of the probability of a failure occurring

- Classification of the severity of the failure on the system

- Identification of any critical items whose failure significantly affects the ability of the system to perform its overall function or significantly affects life cycle costs or safety

- Assistance in defining corrective action

In the FMEA, each component of a system, subsystem, or equipment is subjected to a series of "what if?" questions. The analyst answers these questions by indicating the effect of each failure occurrence mode on system operation and suggests possible techniques for minimizing or eliminating these effects. When the probability of each component failure is estimated, the probability of equipment, subsystem, or system failure can be estimated and the effect of the failure described.

2. When an FMEA Should be Performed

An FMEA provides major input to the design reviews that are conducted periodically throughout the development and construction phases of a project. Because limited design information is available during the conceptual design, an FMEA may be performed at the initial functional level of the equipment or system. As more engineering design information becomes available and as the design progresses, an FMEA can be performed in successively greater detail on lower functional levels. The FMEA can be performed at any time on a new project or existing plant or equipment.

The level to which an FMEA is performed is a function of:

- The detail of information available

- The development or construction phase of the plant or equipment

- The end effect of a failure

- Where the item of interest is located in the functional breakdown structure

- The level to which the design requires verification

3. FMEA Objectives

As a result of an FMEA, failure modes of an operating plant or equipment can be identified, evaluated, and presented in an orderly and organized manner. The analysis aids in verifying the integrity of the design and in identifying design features that minimize or obviate the effects of potential failure modes. Hazards to life, plant, or

equipment operational success can be identified and assessed for individual failure modes. Hazardous failure modes (those with both a high probability of occurrence and a major severity to plant operation) can then be addressed for immediate corrective action.

More realistic engineering estimates (reliability, safety, performance, etc.,) can be made. For example, by knowing the manner in which a failure occurs, engineers can achieve high reliability by considering redundancy at the component or part levels. Redundancy at these levels is not normally considered when estimates and assessments are based on the stress levels only.

4. FMEA Output

The final results of an FMEA are a criticality value for each failure mode at any functional level and a recommendation for corrective action. When the failure mode criticality is known and the need for corrective action verified, management decisions for design review or engineering redesign can be implemented.

In addition, the FMEA information will assist in:

- Establishing realistic guidelines for a program to test and demonstrate "availability factors"
- Establishing criteria to validate availability factors when other data are not available, e.g., failure rates
- Evaluating plant or equipment availability, cost effectiveness, and operational costs
- Establishing data collection guidelines to validate plant or equipment functional characteristics, e.g., reliability, performance, safety
- Identifying high component or part stress levels requiring corrective action, e.g., use of more reliable components, reduction of applied stress, or use of redundant components or parts

C. DETAILED PROCEDURE FOR PERFORMING AN FMEA

1. Procedure

A step-by-step procedure for performing an FMEA is presented in this section.

STEP 1: Determine the Functional Level Breakdown Structure (FLBS)

A Functional Level Breakdown Structure (FLBS) is usually depicted as a functionally-oriented family tree composed of subdivisions of a plant, system, or equipment. The first step in its development is to determine the functional level breakdown of the

largest item, i.e., a plant or major equipment. The plant or equipment is then subdivided into its various systems, then further divided into equipment, assemblies, subassemblies, and parts. The FLBS provides a ready reference to the functional relationships of each item comprising the total plant or system. Figure A-1 illustrates a typical FLBS.

Information used to develop the FLBS is gathered from the engineering data package, engineering design concepts, system functional descriptions, engineering designs, and process descriptions, etc.

The number of successive functional levels identified in an FLBS is a matter of judgment. For example, it should not be necessary to break down an off-the-shelf, commercially available item being used in an assembly.

STEP 2: Identify and Number the Elements of the Functional Level Breakdown Structure (FLBS)

To facilitate the identification of item functions throughout the FMEA and to ensure traceability to all data elements, a consistent and logical coding system is required. The numbering system should uniquely identify the item and reflect its association with items at higher and lower levels.

Described below is a recommended coding system that may be used in performing an FMEA. The decimal-based coding system described provides traceability from the highest to the lowest level in the FLBS.

Each block of the FLBS is assigned a number which is placed in the lower right-hand corner of the block. In this manner, any level can be readily associated with its higher or lower level item and any failure mode can easily be traced within the hardware system structure.

Figure A-1 illustrates the use of this coding system.

LEVEL 0: Project name, e.g., Photovoltaics Test and Applications Experiments

LEVEL 1: A system, plant, or overall function, e.g., Stand-Alone Photovoltaic Power Plant

LEVEL 3: Equipment, e.g., Solar Array

LEVEL 4: Major assemblies, e.g., Solar Sub-array

LEVEL 5: A subassembly of the assembly, Level 4, e.g., Solar Module

LEVEL 6: Parts within a subassembly, Level 5, e.g., Solar Cell

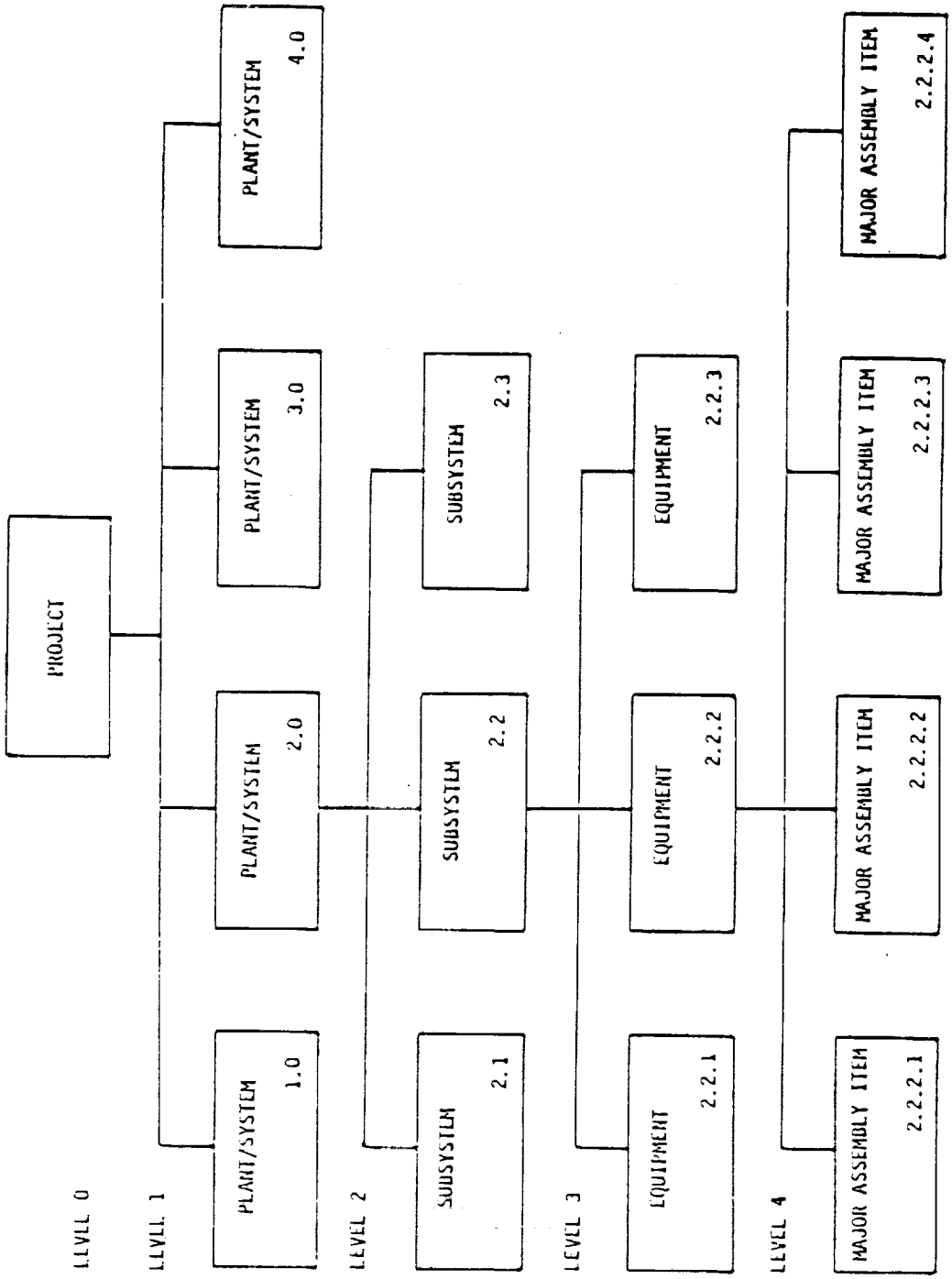


Figure A-1. Example of Functional Level Breakdown Structure.

STEP 3: Develop a Functional Block Diagram (FBD)

The Functional Block Diagram (FBD) is developed from the Functional Level Breakdown Structure. It graphically presents the interfaces among the individual elements of the function being studied. All inputs to and outputs from each element are indicated on the diagram and clearly labeled. Information required to develop the FBD is obtained from the engineering data package. (A block diagram will be developed for each item at levels involved in FMEA). Figure A-2 is an example of an FBD.

The following guide is suggested:

- Define the item function(s) and each element therein
- Ensure that the operation of each element is known
- Illustrate relative position of each element with a block and connect these to illustrate functional relationships
- Identify each block by name and number in accordance with Step 2
- Enter operating and input/output parameters for each element and for the item
- Ensure that the FBD illustrates the functional relationship between each element

The FBD provides a readily verifiable reference list of the functions and specified output of the elements. It can be used in subsequent analysis to:

- Identify inadequate or missing input/output specification requirements
- Identify failure modes
- Derive accurate failure effects definitions
- Verify compliance with specification requirements

STEP 4: Identify and Collect Information Required

In order to fully evaluate the functions, failures, and effects of the system as a whole, and its component elements as developed in the FBD, considerable information may be required. This information can be obtained from the engineering data package, manufacturer's catalogs, functional diagrams, engineering drawings, failure reports, environmental descriptions, etc.

10

Figure A-2. Functional Block Diagram (to be supplied).

Some of the specific elements of information that may be required by the engineer or analyst in completing the FMEA are:

- Generic Name - Common name of the item being analyzed, e.g., power conditioning unit

- Physical Location - Place where the item resides in the facility, such as a building name or number; if a location number is available, include that number

- Manufacturer's Name - Name of the item manufacturer and his item name if that is different from the generic name, e.g., Sunverter

- Model Number - The model number assigned to the item by the manufacturer

- Assembly Drawing Number - From the engineering data package, the engineering assembly drawing number that includes the item

- F/N and Drawing Number - The "find" number used on the assembly drawing for the item being analyzed

- Operating Parameters - Conditions under which the item operates in the system; all items that do not apply should be marked as not applicable (N/A)

- Manufacturer's Specifications - The manufacturer's recommended operating conditions, not to be confused with design operating conditions

- Operating Life Expectancy - Estimation of the item's life in the system

- Maintenance Schedule - The frequency of schedule maintenance for the item

- Power Source - The type of energy used to power the item, e.g., electricity, fuel oil, gasoline, solar flux

- Controls - The equipment that is used to maintain the function within proper operating limits, e.g., motor controllers, voltage regulators

- Switch/Instrument Locations - The location of switches and instruments that monitor and control the item

- Intended Function and Operation - A description of the item, including: the manner in which the item functions within the system; how parts within the item interface with the item; and how the item relates to the system

- Critical Parts - The name of each part that may cause an end item failure or system hazard

- Probable Failure Modes - A description of how each part may fail

- Probable Cause - The probable reason for failure, e.g., poor lubrication, operator error, insulation breakdown, corrosion

- Effect on Item - Conditions that occur in the item when the part fails, e.g., overheating, fire, electric shock

- Interfacing Item - An identification of interfacing components or systems that may be affected by a failure of this item

- Interface Effect - Description of the effect that a failure of this item will have on an interfacing system

STEP 5: Failure Mode and Effects Analysis Worksheet

To facilitate systematic performance of an FMEA and to record the analysis, a Failure Mode and Effects Analysis Worksheet has been designed and is shown in Figure A-3. Instructions for the completion of the worksheet can be used as a guide to the performance of FMEA. For ease of reference, lines and columns of the worksheet shown in Figure A-3 have been numbered.

a. Identification Data

1) Project/Facility - Identify the project facility

2) Level - Enter initial level FLBS number and item name

3) Drawing Number - Insert drawing number of the item

4) Level - Enter next lower level FLBS number and item name

5) Drawing Number - Insert drawing number for lower level item

6) Level - Enter next lower level FLBS number and item name on which the FMEA is being performed, such as: 3 battery bank

7) Drawing Number - Enter drawing number for lower level item

8) Company - Insert name of company conducting the FMEA

9) FMEA Engineer/Analyst - Insert name of the engineer or analyst performing the FMEA

10) Date - Enter date on which FMEA was performed

11) Reviewed by - Insert the name and title of the person within the company who reviews the FMEA

b. Analysis

12) Item Number - Insert FLBS number of item being analyzed

13) Item Name/Function - Insert the name and function postulated to fail

14) F/N (Find Number) - Insert "find" number for item obtained from assembly drawing

15) Operating Parameters - Enter a brief description of the item's parameters obtained from the Item Functional Narrative Description

c. Identification and Traceability. A sequence number is assigned for each failure mode of an item and recorded in the S/N column (Column 16) of the FMEA Worksheet. To maintain complete visibility of each failure mode and its relationship to the system, the failure mode sequence number should be placed in parentheses when associated with an item function number, and shown as:

2.2.1 (2)

This indicates the second failure mode associated with the Level 3 item.

d. Failure Modes. A failure mode of an individual item is postulated on the basis of the stated requirements contained in the equipment specifications and engineering judgment. A "realistically probable" failure mode is one that can cause a deviation from specified output function requirements.

Each output function is evaluated in terms of one or more of these modes; each realistic and probable mode is described concisely in Column 17 - Failure Mode.

e. Probability of Occurrence. Obtaining this value of probability of occurrence of a specific failure mode can be quite difficult, particularly in the earlier phases of project development. However, some measure (or estimate, or even "gut feeling") of this probability is needed to evaluate failure modes. One approach is to use ordinal rankings of the likelihood of occurrence; this naturally leads to the categorizing of like failure probability into groups. Differing analyses have used differing schemes of grouping. One method uses six levels of probability of occurrence ranging from "frequent" to "impossible." However, it might be noted that once a failure mode is adjudged impossible, it needs no further consideration and can be excluded from the analysis. Whatever scheme of probability assessment is used in the FMEA will depend upon the availability of failure occurrence data and specifics of the ranking system used.

14

FAILURE MODE AND EFFECTS ANALYSIS
WORKSHEET

Page _____ of _____
Rev. No. ____ Date _____

PROJECT/FACILITY _____ (1) _____
Level _____ (2) _____
Drawing No. _____ (3) _____
Level _____ (4) _____
Drawing No. _____ (5) _____
Level _____ (6) _____
Drawing No. _____ (7) _____

COMPANY _____ (8) _____
FMEA Analyst _____ (9) _____
Date _____ (10) _____
Reviewed By _____ (11) _____

Item No.	Item/Name Function	F/M	Operating Parameter(s)	S/M	Failure Mode	Failure Symptoms/ Reasons	Item Failure Effect	End Effects and Criticality						Proposed Corrective Action(s) and/or Remarks
								Subsystem		System		Interfacing System		
(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)	(21)	(22)	(23)	(24)	(25)	(26)

Figure A-3. Failure Mode and Effects Analysis Worksheet.
("Clean" copy will be furnished).

f. Failure Symptoms and Methods of Detection. For each failure mode, the analyst determines how a failure will manifest itself, e.g., a change in the recognized functional behavior pattern. Symptoms may be confined to the operation of the specific item under consideration (local) or to be both "local" and "end effect" evidence of failure.

g. Method of Detection. The method of failure detection should be stated. Detection is made possible by features incorporated in the design to monitor and recognize that a failure has occurred or will occur. The early detection of failure is of critical importance if successful operation and output of an equipment or potential personnel hazards are involved. It is of minor importance if impact provisions may be incorporated in the design to detect specific failures before they constitute hazards. Such monitoring devices may be included in various levels related to the criticality of the function.

h. Failure Reasons. The possible reasons for each postulated failure mode will be identified, described, and listed with the symptoms in Column 19. A failure mode can have more than one cause, so all possible independent causes within the next lower levels are to be considered. For example, failure causes at Level 3 are considered when performing a Level 2 analysis. Failure cause identification is an iterative process. When adequate failure cause identification and description cannot be established at the next lower level, the analysis should be continued to a lower level until satisfactory identification and description of failure cause can be determined. Lower level analysis is generally possible as a project progresses through the development and construction phases and more design engineering information becomes available.

STEP 6: Failure Effects

A failure effect is the consequence of each failure mode on an item's operation, function, or status. These effects are identified and recorded in Column 20 on the FMEA Worksheet. The failure effect also impacts on the next higher level, and ultimately may affect the Initial Level under analysis. Therefore, both a local effect and an end effect as well as compensating provisions should be defined and evaluated.

- Local Effects - The consequences of each postulated failure on the output of the item, including second-order effects. The purpose of defining the local effects is to provide a basis for judgment when evaluating existing compensating provisions or formulating recommended corrective action. In some cases, there may be only local effects.

- End Effects - The effects of the postulated failure on the operation, function, or status of the next higher level. These should be assessed concurrently with local effects. The end effect described may be the result of two failures -- for example, the failure of a safety device to function at the same time that item function exceeds design limits. End effects resulting from a double failure should be evaluated and defined on the FMEA Worksheet in the remarks column (Column 29).

- Compensating Provisions - Any internal compensating factors that circumvent or mitigate the effect of the postulated failure. Identification and evaluation of these provisions are necessary to evaluate the true behavior of the item in the presence of an internal failure. Compensating provisions include redundant items that provide continued and safe operation if one or more items fail; alternate modes of operation; safety or relief devices; and any other means, such as monitoring or alarm provisions, that ensure effective operation or reduce damage when failures occur.

STEP 7: Severity of Failure

The severity of each failure must be assigned by the analyst. The criteria used to evaluate severity will differ according to the specific aims of the analysis. For example, a failure that is of high severity to a reliability analyst may be negligible from a safety point of view. In some cases, actual numerical values of the loss can be used as the failure severity, e.g., the value of the product not produced, the cost of repair, etc. However, most frequently, losses are grouped into categories. In most analyses dealing with safety, four levels of severity are used, but the analyst should choose the system of assessing severity most appropriate to his aims and the specifics of the system being studied. As an illustration, the definitions of the categories of severity of loss for systems safety analyses are given:

- Category IV - Negligible: Failure will not result in personnel injury or damage to the system or environment.

- Category III - Marginal: Failure can be corrected or controlled without injury to personnel or major damage to the system or the environment.

- Category II - Critical: Failure will cause personnel injury or major damage to the system or the environment, or will require immediate corrective action for personnel or system survival.

- Category I - Catastrophic: Failure will cause death or severe injury to personnel, system loss, or major environmental damage.

Analogs of the severity categories for system availability, maintainability, etc., can be constructed. The number of categories used depends largely on the amount of information available about the system.

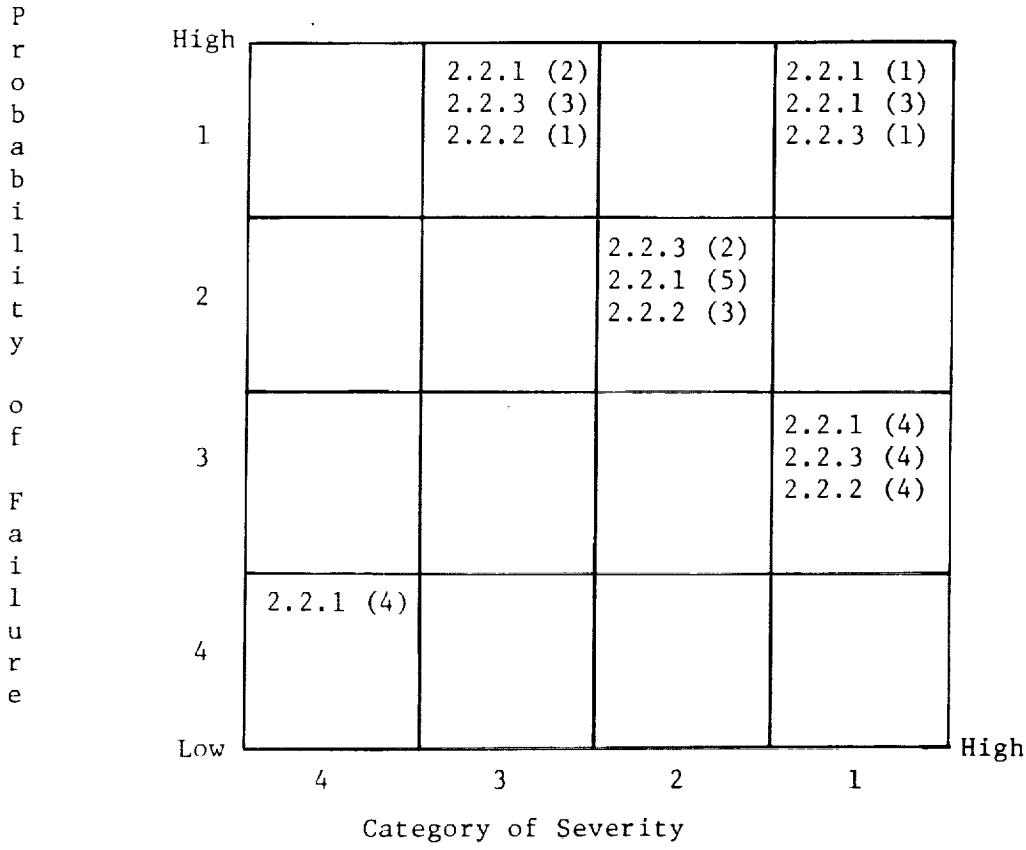
The derived value of severity assigned is the higher level that can be applied to a failure, even if a lower classification is also applicable. This category is entered for each failure reason on the FMEA Worksheet in Column 21.

STEP 8: Criticality Assessment

The assets available to implement corrective actions are limited in any project. Therefore, an effort must be made to prioritize the failures to be corrected. An acceptable ranking measure would be the expected loss due to each failure mode. This is the product of the probability of occurrence of the failure mode and the loss resulting from it, where the loss might be measured in dollars. Then the failure mode with the highest expected loss would receive the rank of highest criticality, and have the highest priority for corrective action. However, the analyst does not usually have actual values for either the loss or the probability of occurrence, but only ordinal rankings or classifications, which cannot be so easily combined. Defining criticality as the product of the rankings of probability of occurrence and severity is a mathematically spurious use of rank order statistics that can lead to mis-prioritizing failure modes, and consequent misuse of corrective action assets.

Schemes do exit for prioritizing failure modes based on ordinal rankings and most rely on the construction of a criticality matrix. An example of a criticality matrix is shown in Figure A-4. In this example, four categories of probability of failure and four categories of severity are used. The failure mode identification number is entered in the appropriate box of the matrix and the criticality of all failure modes can be visualized. This matrix can show dominant failure modes (high probability and severe effect), but rankings modes that are not dominant requires study of the specifics of the failure, both its likelihood and its consequences. Ultimately, engineering judgment must be used to assess the priority of criticality of each failure mode.

Criticality has different effects on various plant or equipment levels. For example, an item may fail in a particular mode; criticality to the item amy be major (the item ceases to function). However, loss of the item may have little or no effect on the subsystem or system. Hence, criticality at the higher level is minor or insignificant. The analyst must, therefore, assess the effect of failure on the item as well as on other levels of the system. The assessed criticality values for item, subsystem, system, and interfacing systems are documented on the FMEA Worksheet (Columns 24, 26, and 28).



LEGEND

Probability of Failure Occurrence	Category of Severity of Failure
1 - High	1 - Catastrophic
2 - Moderate	2 - Critical
3 - Low	3 - Major
4 - Unlikely	4 - Minor

Figure A-4. Illustration of Criticality Matrix.

STEP 9: End Effects and Criticality

When the failure effects of the item have been analyzed and entered in Column 20, the category of Severity of Failure assessed and entered in Column 21, and the criticality assessed and entered in Column 22, the analysis of failure effects is complete. The end effect on the subsystem is concisely described in Column 23, and its criticality value entered in Column 24.

The end effect on the system is described in Column 25, and criticality shown in Column 26.

Interfacing systems affected by the failure should be identified by the FLBS number and entered in Column 27, along with a description of the effect. Criticality should also be computed and entered in Column 28.

STEP 10: Remarks

The analyst is expected to recommend corrective action based on his analysis of failure modes effects and criticality. These recommendations should be noted in Column 29 to clarify any point of the analysis.

STEP 11: Prepare Problem/Failure Report (P/FR)

The final step in the FMEA is to document the corrective actions recommended and provide a mechanism for management follow-up to ensure that they are implemented. The Problem/Failure Report provides such a mechanism.

The purpose of the Problem/Failure Report is to:

- Summarize identified failure modes
- Identify the failure mode location through the FLBS number
- Summarize effects of failure on item, subsystem, system, and interfacing systems
- Tabulate and rank failure modes according to criticality value
- Identify and document recommended corrective actions
- Document actions taken to implement corrective action
- Periodically document the status of implementation of actions by P/FR status reports.

Project management should require periodic updates of P/FR Status Reports on the progress of corrective actions. These reports should be closed out.

20

STEP 12: Prepare the FMEA Report

After an FMEA has been completed, it is essential that a technical report be prepared to document the detailed data, analysis, findings, and status of recommended corrective actions. This report should be distributed to appropriate management and engineering personnel within the company and to other personnel involved with project design review.

D. SUMMARY

This procedure has established the steps necessary to perform a Failure Mode and Effects Analysis (FMEA) on an item at any level. Specifically, this procedure:

- Provides a technique for performing a thorough analysis that can identify engineering and technical problem areas and failure modes at specific plant levels, and contribute to the validity of the design review process

- Provides an analytical technique that can identify necessary corrective action, and presents the information so that top management can make management and technical decisions which, when implemented, can improve the safety of plants and equipments, can reduce or eliminate plant and personnel hazards, improve efficiency and effectiveness, and reduce life-cycle costs.

DEFINITIONS

The following definitions are pertinent to a Failure Mode and Effects Analysis:

- Critical Item - An item which, if it fails, will cause the shutdown of an entire system or plant, or pose a threat to life

- Criticality - Estimated measure of the failure mode impact on an item; it is derived by considering the possibility of occurrence of a failure mode with its severity

- Criticality Matrix - A method used to combine the probability of failure occurrence with the category of severity to provide a relative value for criticality

- End Effect - The impact of a failure mode on the operation, function, or status of the next higher-level item, e.g., the failure of an equipment or subsystem

- Equipment - Two or more functional assemblies operating cooperatively to produce a functional objective or output

- Failure - Non-performance of a specified function

- Failure Cause - A defined condition associated with a failure

- Failure Effect - The resultant condition of a failure on an item's function, operation, or status. Failure effects may be classified as local effect or end effect

- Failure Mode - The manner in which a failure occurs. Failure modes can be classified in one of four ways:

  - Premature operation of an item

  - Failure of an item to operate at a prescribed time

  - Failure of an item to cease functioning at a prescribed time

  - Failure of an item to function at a specified level during operation

- Failure Mode and Effects Analysis Worksheet - A form for consolidating an item's function, level, failure symptoms, failure mode, effect, severity, and criticality. It is the basis for identifying corrective action and making recommendations for using the FMEA output

- Functional Block Diagram - A graphic representation of how the individual elements of a function relate; all inputs to and outputs from each element are identified

- Functional Level Breakdown Structure - A functional diagram composed of subdivisions of a system plant, or equipment; it depicts in successive levels the relationship of individual assemblies, equipment, and their component parts

- Initial Level - The highest level upon which the FMEA is to be performed

- Interface - The relationship of an item's functional output to the input of an associated item

- Item - An item may be a system, subsystem, equipment, component, or part

- Item Narrative Functional Description Form - A form for a narrative description of an item's physical and operational characteristics

- Level(s) - The relative complexity of a plant, system, assembly, or function. The levels progress from the complex (project) to successively lower breakouts of items

- Local Effect - The impact of a failure mode on the item being analyzed

- Operating Parameters - The normal and acceptable range of the physical and operational characteristics within which an item functions (not the manufacturer's specification limits)

- Severity - A qualitative measure assigned to each failure effect based on its impact on the operational functioning of the item

- Subsystem - A subsystem is composed of two or more equipments operating cooperatively to achieve a functional objective or output

- System - A system is composed of two or more functional subsystems operating in a cooperative manner to achieve a functional objective or output

APPENDIX B

PROCEDURE FOR PERFORMING A HAZARDS ANALYSIS

A. INTRODUCTION

1. General

This "Procedure for Performing a Hazards Analysis" is provided by the DOE Photovoltaic Lead Center as a guide to aid contractors in performing a Hazards Analysis and as an informative document for the field center project managers. It is not intended to impose this document as a contractual requirement, but rather to illustrate a systematic method for performing a Hazards Analysis in order to assure safety in the design and deployment of systems and equipments.

The scope of Systems Safety excludes industrial safety, which is concerned with the job-site safety of personnel and the compliance of work areas with federal, state and local code.

Hazards Analysis, as addressed in this procedure, is a major element of a total System Safety program, and complements procedures for Failure Mode and Effects Analyses and other System Safety activities. This procedure defines the overall concept of Hazards Analysis, i.e., what is a Hazards Analysis? When is a Hazards Analysis required? It provides a recommended methodology for Hazards Analysis, and the reporting of results to management for necessary actions.

B. APPLICATION

1. Scope

The objective of the Test and Applications (T&A) subprogram is to obtain operational experience with complete photovoltaic systems in a range of applications. The main thrust of the T&A subprogram will be directed toward a carefully selected series of experiments in remote, residential, intermediate load center, and central station applications. In the latter three experimental areas, interaction with electric utility generation-transmission-distribution grids will be emphasized. Inherent in all photovoltaic T&A projects is the need to ensure that safety is designed into the system. As part of a methodical approach to system safety engineering, hazards associated with each system, subsystem, equipment, and component must be identified, evaluated, and either eliminated or controlled to an acceptable level. The timely detection of these hazards is cost-effective not only from the standpoint of design and development but also on a life-cycle basis. System hazard points must be described and documented.

2. Hazards Analysis Defined

Hazards analysis as considered in this procedure is a systematic process for examining the functional interrelationships of a system to establish the following:

- Identify hazards, determine corrective actions, and establish corrective action priorities
- Assess the injury or damage that is associated with each hazard and the probability that it will occur
- Determine which hazards can be prevented either through modification of a design or by changing procedures associated with its use
- Determine methods to control those hazards which cannot be eliminated from the system by changes in design or procedure
- Assess the risk associated with operating or using the system after it has been determined that hazards be eliminated or controlled
- Determine those hazards for which it is desirable to establish and monitor an alarm system
- Determine and assess those hazards, e.g.:

- Excessive noise levels
- Inadvertent release of kinetic energy
- Inadvertent release of potential energy
- Exposure to excessive heat or cold

3. When is a Hazards Analysis Required?

Hazards analyses are performed at appropriate phases of system development to ensure that hazards are recognized and controlled, that hazards have not been overlooked, and that new hazards are not created.

a. Conceptual Design - A preliminary hazards analysis is performed early in the conceptual phase of the project so that safety considerations are included in tradeoff studies and design alternatives. Based on the best available data, hazardous conditions associated with proposed design or function are evaluated for hazards probability, hazard severity, risk, and probable operational constraints. Safety provisions needed to eliminate or control hazards are identified and used in preparing performance and design specifications. This preliminary hazards analysis establishes the framework for further hazards analyses and for safety engineering evaluation of system design.

b. Preliminary and Detail Design - During these phases, the design of system components progressively becomes more specific. Based on the preliminary hazards analysis, the engineer can establish both generic and specific safety criteria to aid the design effort (e.g., "all pressure vessels shall have a vent or bleed valve."). The preliminary hazards analysis then is replaced by final hazards analyses performed at increasing levels of design detail and design maturity. The results of these analyses are major inputs to the in-house design process documented through these expanded efforts.

c. Subsystem Hazards Analysis - A subsystem hazards analysis is performed to identify hazards within the level of the subsystem and within the function of the subsystem. This analysis identifies all components and equipments whose performance, performance degradation, functional failure, or inadvertent operation could result in a hazard. It includes a determination of the failure modes and the effect on safety when failures occur in subsystem components. The subsystem hazards analysis should begin as soon as actual design of the subsystem has been developed and continue as more detailed design information becomes available.

d. System Hazards Analysis - A system hazards analysis is performed on subsystem interfaces to identify hazards above the subsystem level and within the functions of the total system. It examines the effect of subsystem hazards on the whole system. Such analyses should also begin with design and include a review of subsystem interrelationships for:

- Compliance with safety criteria
- Possible, independent, dependent, and simultaneous failure that presents a hazardous condition, including failure of safety devices
- Degradation from normal operation of the safety of a subsystem or the total system
- Changes that occur within subsystems, so that the system hazards analysis can be updated accordingly

e. Construction, Operation, and Maintenance - Operating and support hazards analyses are conducted prior to, and during, the operation and maintenance phase. They are oriented to development and operational testing to identify hazards and determine safety requirements for personnel, procedures, and equipment during these phases. Engineering data, developed from the engineering design and initial test programs, and preliminary hazards analyses are used to support these analyses. Results provide the basis for:

- Identifying hazardous time periods for equipment operation, and the actions required to minimize risk during this time

- Identifying requirements for safety devices and equipment, as well as the monitoring procedures needed to detect functional failure

- Developing warnings, cautions, and enhancing the safety of procedures used in operation and maintenance

- Developing special procedures for handling, storage, transportation, and maintenance

- Establishing requirements for contingency plans and procedures

C. CRITERIA

The requirement for the contractor to perform a Hazards Analysis on new contracts will normally be an inherent part of the contractor's System Safety Program Plan provided in response to Photovoltaic T&A contractual requirements.

Existing contracts may be modified to require submittal of a System Safety Program Plan incorporating the requirement to provide a Hazards Analysis at the discretion of the DOE program manager. This decision will be influenced by the size, complexity, and amount of work remaining on the project under consideration and also by the benefit that will be obtained.

D. PROCEDURE - PERFORMING THE HAZARDS ANALYSIS

This section provides a step-by-step procedure for conducting a hazards analysis, using a hazards analysis worksheet (Figure B-1), for performing and documenting the analysis. The following describes the worksheet and discusses pertinent input data, analysis techniques, hazards identification and descriptions, severity and probability, and corrective action measures. For convenience, pertinent lines and columns on the form in Figure B-1 have been coded and each will be discussed.

1. Input Data

Hazards Analysis data is obtained from analysis of available design data and experiences. These data include:

- Mishap and accident reports

- Mishap probabilities from safety reports

- System safety analyses

- Failure mode and effects analyses

- Fault tree analysis

Page (9) OF
REV. NO. (10) DATE (11)

(1)

PROJECT/FACILITY (2)
Level (3)
Drawing No. (4)
Level (5)
Drawing No. (6)
Level (7)
Drawing No. (8)

RISK ASSESSMENT VALUES	
Severity	Probability
I. Catastrophic II. Critical III. Marginal IV. Negligible	1. Frequent 2. Probable 3. Occasional 4. Remote 5. Improbable

Company (12)
Hazards Analyst (13)
Date (14)
Reviewed by (15)
Type of Hazards Analysis (16)
Project/Program Development Phase (17)

(18)	HAZARD DESCRIPTION (19)	STATE (20)	CAUSE (21)	EFFECT (22)	INITIAL RISK SEVERITY (23)	INITIAL RISK PROB. (24)	RECOMMENDED CORRECTIVE ACTIONS (25)	FINAL RISK SEVERITY (26)	FINAL RISK PROB. (27)

Figure B-1. Hazards Analysis Worksheet.
("Clean" copy will be furnished).

5230-3 Use. 5

- Failure probabilities from reliability analyses
- Test results from test programs
- Human-factors data from human factors studies
- Functional breakdown structures from project management plans
- Item functional narrative descriptions from energy management plans
- Problem/failure reports from reliability analyses

Figure B-2 illustrates the numerous sources of data used in performing hazards analysis.

2. Identification and Administrative Data

Lines 1 through 17 on the worksheet identify the item being analyzed, provide a means of relating it to other items, and provide references:

Line 1 - Insert the name of the item (system, subsystem, equipment, etc.) on which the analysis is performed.

Line 2 - Insert project name or facility.

Lines 3, 5, and 7 - Insert the functional breakdown structure identification of the item. The development and codification of a functional breakdown structure has been described in the procedure for performing a failure mode and effects analysis.

Lines 4, 6, and 8 - Insert drawing or specification numbers associated with the item.

Line 9 - Insert page number.

Line 10 - Insert 0 for the initial hazards analysis. The letters A, B, C, D, etc., are used to designate subsequent analyses.

Line 11 - When a prior analysis is revised, insert the date of the revision.

Line 12 - Insert name of company or government agency performing the analysis.

Line 13 - Insert the name of the individual responsible for conducting the analysis.

Line 14 - Insert the date of the initial hazards analysis.

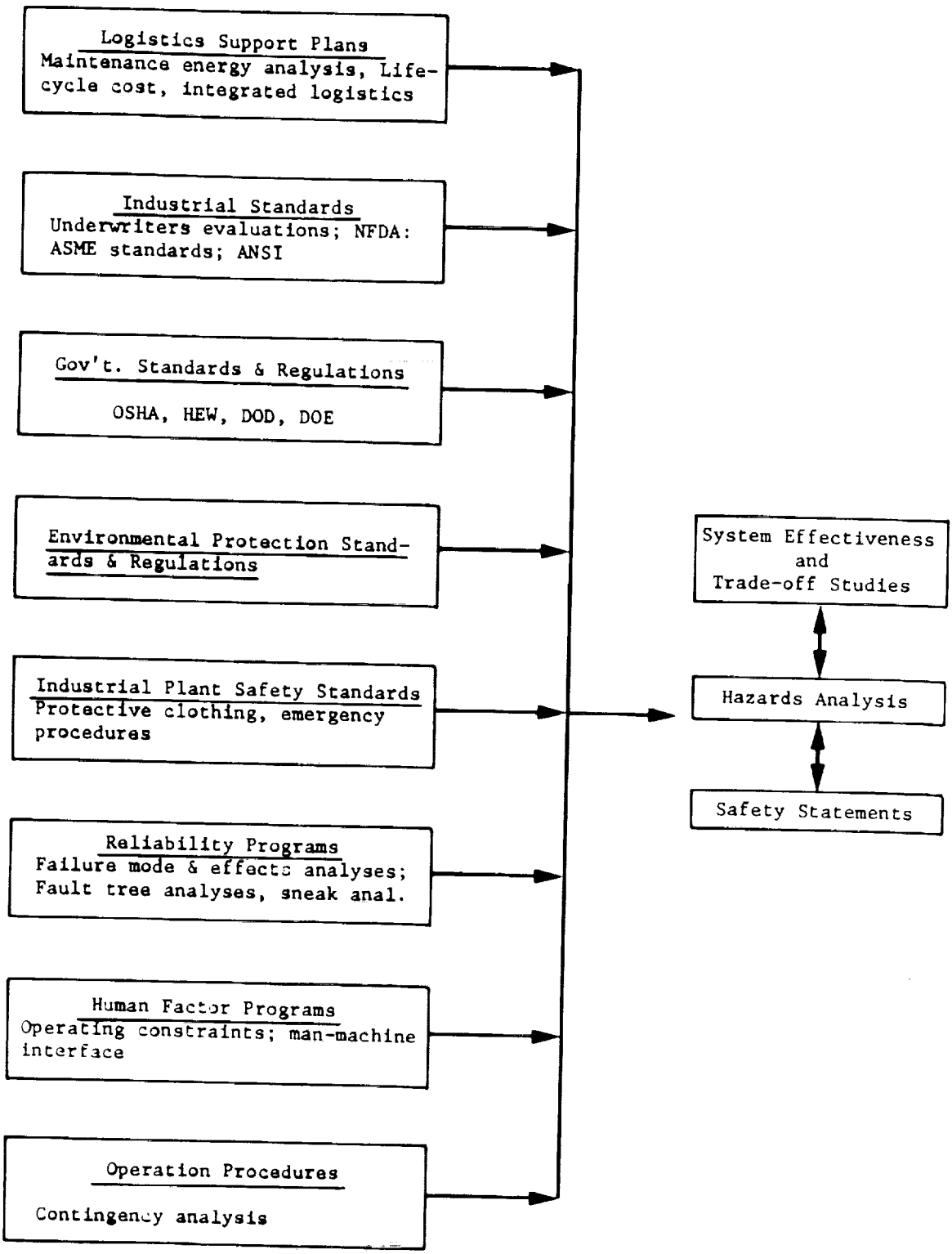


Figure B-2. Some Data Sources Used in Conducting a Hazards Analysis.

Line 15 - Insert the name of the individual reviewing or approving the analysis.

Line 16 - Insert type of analysis, e.g., preliminary hazards analysis; subsystem hazards analysis; system hazards analysis; or operating and support hazards analysis.

Line 17 - Insert project development phase, e.g., concept, design, development, construction, demonstration, or operation. The development phase of the project relates to the type of hazards analysis (Line 18) and the revision number (Line 12).

3. Analysis Techniques

The selection of a specific method of analysis is based upon the level of complexity of the plant, system, or equipment under consideration, the level of the item within the functional breakdown structure (FBS), and the status of system development. The technique selected must allow for continuity through the system life-cycle. It should also permit coordination of analysis results to ensure that hazards are removed or minimized.

Hazards analyses may be either qualitative or quantitative. Models and techniques should be compatible with those being used by other disciplines, e.g., reliability, human factors. Analysis techniques may be inductive or deductive. For example:

- An inductive method such as fault hazard analysis can be a qualitative or quantitative analysis. It requires investigation of the subsystem to determine hazard modes, causes, and effects. A failure mode and effects analysis provides most of this information.

- A deductive method such as fault tree analysis is used to analyze all events, faults, and occurrences and their combinations that could cause or contribute to the occurrence of a defined undesired event. A qualitative or quantitative analysis may be conducted. A logic diagram (fault tree) is used to analyze undesired events. This analysis identifies all events and combinations of events that can result in the specific undesired event. Mathematical techniques have been developed for combining and simplifying probabilities and quantitative evaluation.

4. Hazard Identification

Hazards analysis is undertaken to identify hazards and either eliminate the cause or minimize the effect. Depending on when the analysis is performed, it should identify and assess:

- Hazardous components (e.g., energy sources, fuels, battery acids, high voltage, and pressure systems).

- Safety-related interface considerations among various elements of the system (e.g., material compatibilities, inadvertent activation, fire/explosion initiation and propagation, degradation in the safety of a subsystem or the total system from normal operation of another subsystem).

- Environmental considerations, including the normal operating environment (e.g., drop, shock, extreme temperatures, noise and health hazards, fire, electrostatic discharge, lightning, radiation).

- Operating, demonstration, maintenance and emergency procedures (e.g., human error analysis of operator functions, tasks, and requirements; effect of environmental factors such as equipment layout and lighting on human performance; life support requirements and their safety implications, crash safety, egress, rescue, survival, and salvage).

  Facilities, support equipment, and training (e.g., provisions for storage, assembly, checkout, proof-testing of hazardous systems/assemblies which may include toxic, flammable, explosive, corrosive or cryogenic fluids; electrical power sources; training and certification pertaining to safe operation and maintenance).

- Safety-related equipment and safeguards, and possible alternative approaches (e.g., interlocks, system redundancy, fail/safe design consideration, subsystem protection, fire suppression systems, and personal protective equipment).

- Hazardous time periods and the actions needed to minimize risk during this time.

- The need for design changes to eliminate or control hazards.

- Requirements for safety devices and equipment and maintenance procedures needed to detect their functional failure.

- The need for warnings, cautions, and special emergency procedures for operating and maintenance.

- The need for special procedures for handling, storage, transportation, maintenance, and modification.

- Compliance with safety criteria.

5. Describing the Hazard

Analysts identify system hazards by responding to "what if?" questions geared to the system. Responses isolate hazardous conditions, their causes and effects, and determine the state of the system when hazards would occur. To assist in the analysis, a list of "standard" types of hazards within the particular project should be developed. This list, modified as required, plus a list of generic hazards, e.g., explosion, toxic vapor release, etc., should provide sufficient descriptive terminology. Identified hazards and related findings are entered in Columns 18-22 on the worksheet shown in Figure B-1.

- Column 18 - This is a number assigned to a hazard within the functional level being analyzed. When added at the end of the functional breakdown structure identifier developed during a failure mode and effects analysis, it uniquely identifies a hazard.

- Column 19 - Enter a brief description of the hazard developed from the analysis.

- Column 20 - Insert the "state" or condition of the item when the hazard exists. Typical states would include test, standby/waiting, operation, maintenance, etc. Hazards can exist in one or more states with the probability of occurrence changing as the state changes. For example, in a test state where normal operating standards may be far exceeded and protective devices not operating, the probability and severity of an accident are far greater than normal; in normal operation, protective devices, pressure controls, or operating conditions would reduce the probability of occurrence and could reduce severity as well.

- Column 21 - Insert the fundamental cause of the hazard or the events which lead to the hazard. General descriptions such as mechanical failure, or radiation are acceptable in initial hazard analyses. However, action needed to prevent the hazard requires a precise detail for action to be taken. For example, the cause of a pressure vessel rupture might be overpressurization, wall corrosion and deterioration, or metal fatigue.

- Column 22 - Insert the effect of the hazard on personnel or system safety. This can be determined from failure mode and effects analyses, fault tree analyses, and system functional specifications or other analyses. There are a number of ways a hazard can affect a system. It can:

  - force a contingency mode of operation which may or may not degrade system operation

- force an abort of system operation

- require an abort that is precluded because no total system loss or fatal injury occurs. The system may still partially function but in a degraded mode or reduced capacity.

6. Hazard Severity

Hazard severity, qualitative measure of a hazard's impact on the system and the personnel involved, is entered in Column 23. Severity values are based on the following categories:

Category I - Catastrophic. May cause death or system loss.

Category II - Critical. May cause severe injury, severe illness, or major system damage.

Category III - Marginal. May cause minor injury, minor illness, or minor system damage.

Category IV - Negligible. Will not result in injury, illness, or system damage.

Hazard severity categories may require adaptation to the particular program under review and may include definite transition points between categories. More specific definition of the degree of injury or damage may also be required.

These categories are particularly useful in evaluating the results of the preliminary hazards analysis. They establish a priority for minimizing or eliminating hazards during the design phase and provide data needed for the more detailed subsystem and system hazards analyses.

7. Hazard Probability

The probability that a hazard will result in an accident during the life of the equipment may be described as "potential occurrence per unit of time, events, populations, items or activities." Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process; a qualitative hazard probability may be derived from analysis and/or evaluation of system safety data obtained from a similar plant, system, or equipment. Supporting data for assignment of hazard probability is listed in hazards analysis reports. Qualitative hazard probability rankings are assigned as follows and entered in Column 24.

DESCRIPTIVE WORD	VALUE	SPECIFIC INDIVIDUAL ITEM FREQUENCY
Frequent	1	Likely to occur frequently
Probable	2	Will occur several times in life of an item
Occasional	3	Likely to occur sometime in life of an item
Remote	4	Unlikely that this hazard will be experienced
Improbable	5	Probability of occurrence is almost nil

NOTE: Hazard severity and probability of occurrence are combined in the Hazards Analysis Report to form an "initial risk assesment" value. This value establishes priorities for corrective action and resolution of identified hazards (D.9.b Item 4).

8. Corrective Action

Corrective actions to eliminate or minimize hazards revealed by analyses should be developed and entered in Column 25. If catastrophic and critical hazards cannot be eliminated or controlled at an acceptable level, alternative measures should be developed immediately. The following order of precedence for corrective actions is suggested.

- Design to eliminate hazards. If an identified hazard cannot be eliminated, control it through selection of design alternatives.

- Control hazards at acceptable levels. Hazards which cannot be eliminated through design selection must be controlled through use of fixed, automatic, or other protective safety features or devices. Periodic assessment of safety devices will be made.

- Detect and warn. When neither design nor safety devices can effectively eliminate or control an identified hazard, special devices to detect the hazard and generate an adequate warning signal should be installed. Warning signals should be designed to elicit appropriate reactions among personnel and should be standardized within like types of system.

35

- Develop procedures and training. Where it is impossible to eliminate or adequately control a hazard through design selection or use of safety and warning devices, safety procedures and training should be used to control the hazard. Procedures should include the use of personal protective equipment. Certification of personnel proficiency in performing safety critical tasks and activities may also be necessary.

- Column 25 - Describe the recommended corrective action. Corrective action will vary according to such factors as severity of injury or damage, the probability of occurrence, and the effort (including cost) required to take preventive action. The action recommended can vary from modification of a maintenance or operating procedure to extensive modification or redesign of the system.

- Column 26 and 2 - Enter the category of severity and probability of occurrence assessed on the basis of the corrective action described in (27). For example, an eye hazard because of machine operation (metal chips) was initially classified as a critical category (II) of severity, with a probability of occurrence of (1); While the hazard may not be eliminated, it is reduced by use of protective eye shielding; the corrective action is to wear an eye shield at all times. As a result of the corrective action, the hazard is reclassified as a category (IV) and the probabability of occurrence, (4), remote.

9. Hazard Analysis Reporting

A Hazard Analysis Summary/Status Report should be prepared periodically to summarize for management the results of the analysis, corrective action taken or recommended, and the status of ongoing corrective action.

The hazards analysis worksheet provides information for the report that will be used by design engineers and management in assessing system safety.

a. Purpose of the Report

1) Summarize identified hazards

2) Rank the hazards by risk values

3) Identify and record recommended corrective actions to eliminate (or reduce) the hazards

4) Document steps taken to implement corrective action

5) Provide status of corrective actions

b. Preparing the Report. The Hazards Analysis Summary/Status Report, Figure B-3, should be completed according to the following guidelines.

1) Insert the name of the item, subsystem or system which has been analyzed.

2) Enter a sequence number for the hazard, e.g., number 1, 2, 3, 4, etc. Hazards should be listed according to their risk value. For example, high-risk hazards (values 1-3) would be listed first with others listed in descending order of risk value.

3) Enter the identified hazard. The hazard listed is obtained from the hazards analysis worksheet (21), and each hazard on the worksheet must be listed in the Hazards Analysis Summary/Status Report. The hazards will not be in the same order as on the worksheet since they must be listed in descending order by risk value. It is not necessary to write as detailed a description as on the worksheet; a brief identification of the hazard is sufficient.

4) Insert the initial risk assessment value obtained by multiplying the category of severity by the probability value in columns (25) and (26) of the worksheet. This value provides a relatively simple way of ranking hazards for management action. These values can be categorized as:

Category	Risk Value	Assessment
High	1-3	Requires urgent attention. Hazard is likely to occur and can result in loss of life and/or system.
Moderate	4-8	Requires attention. Hazard can reasonably be expected to occur with injury and/or major system damage. Costs of injury and system downtime will exceed acceptable standards.
Low	9-12	If hazard occurs it may cause minor injury or system damage. Costs of injury and system downtime are at or below maximum acceptable standards.
Insignificant	13-20	Little chance of hazard occurring. If it does there will be minimal impact on system or personnel. Corrective action recommended only if time and funds are available.

(1)
(Item, Subsystem, System)

Page ____of____
Date _____

Sequence Number	Hazard Description	Initial Risk Assessment	Recommended Corrective Action	Status of Corrective Action	Final Risk Assessment
(2)	(3)	(4)	(5)	(6)	(7)

Figure B-3. Hazards Analyis Summary/Status Report.
("Clean" copy will be furnished).

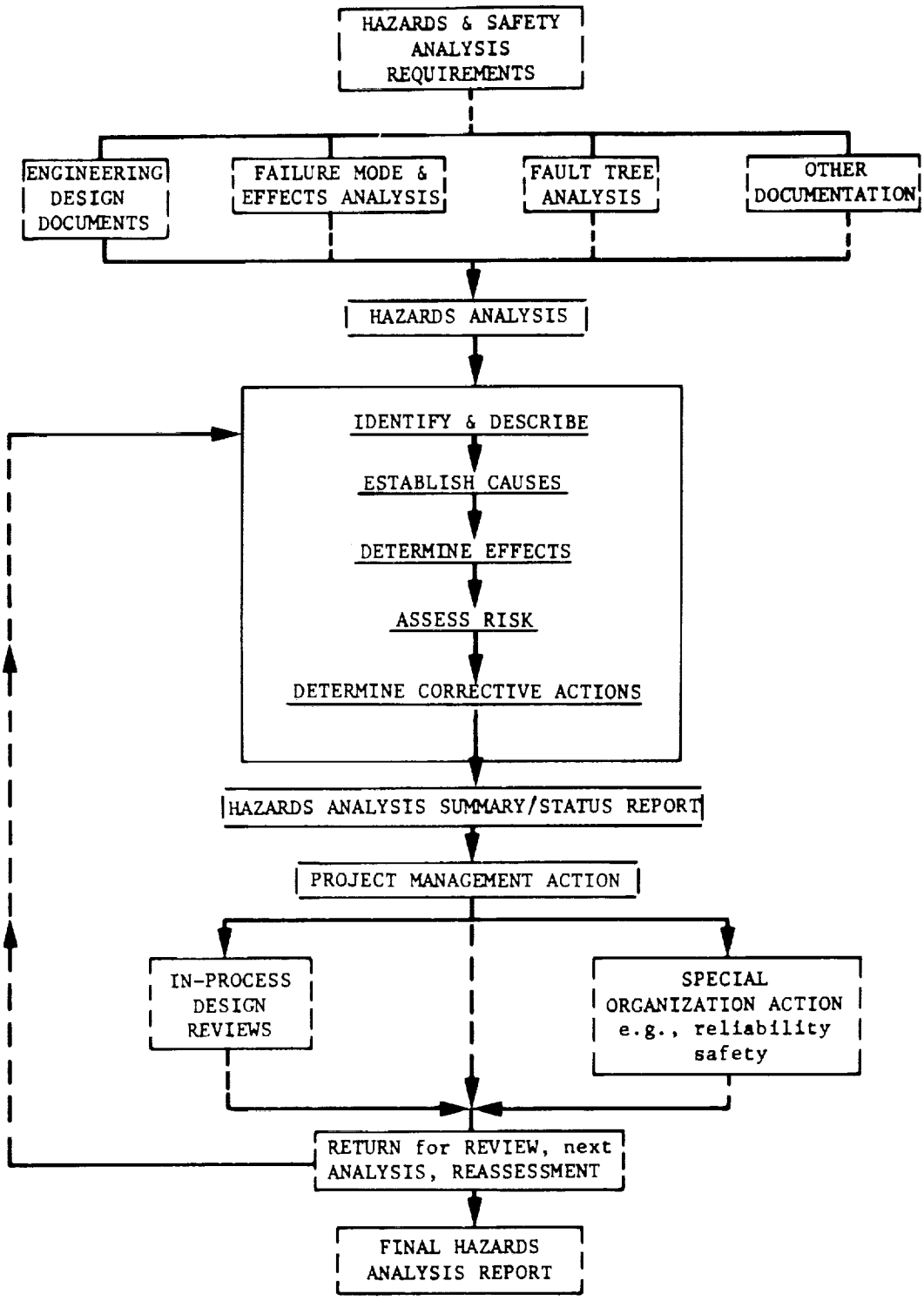


Figure B-4. Hazards Analysis Flow Diagram

5) Describe recommended corrective action. This description, although brief, should coincide with the corrective action recommended on the hazards analysis worksheet, Column 27.

6) Describe the status of corrective action. The description should be sufficiently detailed so that a risk assessment value can be set.

7) Enter a final risk assessment value based on the status of the corrective action. The final risk value should be higher than the initial risk value if the hazard has truly been eliminated or reduced to an acceptable level and system safety obtained.

DEFINITIONS

The following definitions are pertinent to a Hazards Analysis:

- Accident - Any unplanned/undesired event that results in personal injury, death, and/or property damage or equipment loss.

- Failure Effect - The impact of a failure mode on the operation, function, or status of higher-level items (e.g., the failure of an equipment on a subsystem, or upon successively higher levels). The impact may have a "local effect," involving only the failed item, or an "end effect" involving an element of the system or its environment.

- Equipment - Two or more functional assemblies operating cooperatively to produce a functional output.

- Failure - Mal-performance of, or inability to perform, a specified function.

- Failure Cause - A defined condition that results in a failure.

- Failure Mode - The manner in which a failure occurs, e.g., "valve fails to open," "loss of power," "short circuit," or "open circuit."

- Failure Mode and Effects Analysis - A technique for evaluating and documenting the manner in which components or systems fail and determining the impact of the failures.

- Fault Tree - A logic diagram that graphically displays all the potential events and event interactions that can lead to an undesired event.

- Fault Tree Analysis (FTA) - An analysis of an undesired event, by means of a fault tree, to determine the likeliest sequence of events leading to the undesired event, and to develop controls to prevent the undesired event.

- Functional Level Breakdown Structure - A structure diagram composed of functional subdivisions of a system, plant, or equipment; it depicts in successive levels the relationship of individual assemblies, equipment, and their component parts.

- Hazard - Any actual or potential condition that can result in, or contribute to, an accident (e.g., the presence of fuel in an undesired location is a hazard; the fuel iteslf is not).

411

- Hazard Severity - A qualitative assessment of the worst potential consequence of a hazard. Severity is defined by the degree of injury, illness, property damage, or equipment damage that would result from an accident caused by the hazard.

- Level(s) - The physical and/or functional level of organization of elements in a plant, system, assembly, or function. The levels range from more complex to simpler divisions, i.e., system, subsystem, equipment, component, or part.

- Safety - Freedom from unacceptable risks to persons, property, or the environment, or the capability for dealing with all such risks.

- System - A system consists of functional elements (e.g., personnel, procedures, and physical resources) integrated in a cooperative manner to perform its intended function(s).

- Subsystem - A subsystem is an element of a system which performs a function to support a system.

- System Safety Engineering - An element of system engineering which applies specialized professional knowledge, skills, and techniques to identify, eliminate, or control systems hazards.

- Undesired event - A significant event that is detrimental to system operation such as an accident, a potential accident, a power outage, etc.

APPENDIX C

PROCEDURE FOR PREPARING A SYSTEM SAFETY AUDIT

A. INTRODUCTION

This procedure for preparing a System Safety Audit Procedure is provided by the DOE Photovoltaics Tests and Applications (T&A) Lead Center as a guide to aid contractors in preparing a System Safety Audit Procedure as required by DOE contracts and as an informative document for the field center project managers. It is not the intent to impose this document as a contract requirement or to replace or radically alter the contractor's existing audit procedures that are being successfully implemented on Photovoltaics T&A programs. This procedure simply provides a systematic approach for the contractor to use in preparing or modifying his existing system safety audit procedure so that when implemented along with other performance assurance plans and procedures it will strengthen and improve the Photovoltaics Program.

This procedure defines typical requirements and provides examples of documentation required in a system safety audit as it progresses through the stages of familiarization, on-site examination, evaluation, and reporting on the operation of a system.

This procedure will enable the contractor to prepare his system safety audit procedure by describing how he will meet the appropriate requirement of the typical audit plan and also the requirements of his system safety program plan.

B. APPLICATION

The objective of the T&A subprogram is to obtain operational experience with complete photovoltaic systems in a range of applications. The main thrust of the T&A subprogram will be directed toward a carefully selected series of experiments in remote, residential, intermediate load center, and central station applications. In the latter three experimental areas, interaction with electric utility generation-transmission-distribution grids will be emphasized. Inherent in all photovoltaics T&A projects is the need to ensure that safety is designed into the system. As part of a methodical approach to system safety engineering, audits should be conducted to verify that system safety has been adequately addressed during project design and development. These audits should assess areas such as system safety activities, operating procedures, maintenance quality, training, and when necessary, system safety enforcement. The audit enables the field center project managers, along with contractors and other project personnel, to determine the effectiveness of any safety features incorporated in the plants, systems or equipment, and also through the audit report provides the basis for followup to ensure necessary corrective action.

C. CRITERIA

The requirement for the contractor to perform system safety audits will normally be incorporated in all approved contractor system safety program plans as part of the photovoltaics T&A contract requirements. Existing contracts for photovoltaics projects may be modified to require submittal of a system safety program plan incorporating audit requirements. Such a decision will be at the discretion of the field center project manager and will be influenced by the amount of work remaining on the project being considered and also by the benefit that will be obtained.

D. PROCEDURE FOR PREPARING SYSTEM SAFETY AUDIT PROCEDURE

1. General

This procedure describes the approach the contractor may take in preparing his system safety audit procedure for any photovoltaics T&A program. The procedure consists of two basic steps:

a. Review the specifications contained in the contract and also the contractor System Safety Program Plan and determine what he, as the contractor, will do to meet these requirements.

b. Using the typical audit procedure requirements (paragraph 4, below) as a guide, prepare an audit procedure including the requirements from step a., above.

2. System Safety Program Plan Requirements

The contractor should review his approved System Safety Program Plan which describes "what" he will do to meet the contractual requirements and to satisfy his basic obligation to provide an economical and effective safety plan that will meet the needs of the project. The contractor should now determine "how" he will implement a system safety audit that will meet the requirement of his Systems Safety Plan.

3. System Safety Audit Procedure

Paragraph 4 provides the typical requirements for a Photovoltaics Program safety audit. The contractor should review these requirements and in conjunction with the requirements established in the previous paragraph, provide an audit procedure that describes "how" he will meet these requirements. The contractor should be aware that the typical requirements in paragraph 4 are provided only as a guide and it is still the contractor's responsibility to provide an audit procedure that meets all contract and project requirements.

4. Typical Requirements - System Safety Audit

a. Responsibility. The overall responsibility for the system safety audits should be established for each type of audit, i.e.,

- Preliminary Audit - An audit conducted after design and layout concept are completed and technical feasibility of the project is established, but before commercial-type components are combined into a small model pilot plant.

- Special Audit - An audit conducted if test programs or engineering studies indicate that a major design modification requires further evaluation, if a system safety problem cannot be resolved or corrected, or as otherwise directed or specifically indicated.

- Major Audit - An audit normally conducted after completion of subsystem testing, but prior to the startup of a demonstration plant.

This assignment of responsbility is especially important since the contractor may be assigned a supporting role in certain audits; for example, a special audit initiated by the field center project manager or a major audit initiated outside of the project. In addition, the person or organization responsible for initiating appropriate corrective action after each audit must be clearly defined.

b. Audit Team - The method for selecting the audit team, notification of team members, technical expertise required, the number of team members, designation of a team leader or audit chairman, and distribution of audit reports should be described. The audit team may be composed of engineers/process designers, and technical specialists with diverse experience in materials engineering, production or fabrication, reliability, quality, etc., or the audit may be performed by a single auditor. See Figure C-1 for participation request form.

c. Schedule - A master schedule is usually required for all audits. This schedule should be updated periodically to reflect major project milestones, design reviews, etc., and should include type of audit, i.e., preliminary, special or major, the location of audit, and date. Normally, a major audit will be scheduled at least once before commercialization while the frequency of the other audits will vary with project complexity, criticality, etc.

d. Audit Preparation

1) System Safety Audit Agenda. An audit agenda should be prepared which describes the type, project phase, and the scope of the audit to be conducted. It should also list the areas of technical specialization required for the audit. The form shown in Figure C-2 may be used for all audits to delineate audit team membership by areas of specialization.

45

(date)

xxxx
xxxx
xxxx
xxxx
xxxx
xxxx

Subject: REQUEST TO PARTICIPATE AS A MEMBER OF A _____ SYSTEM SAFETY AUDIT TEAM

Reference: Project: _____

Dear xxxx,

In recognition of your technical abilities and experience in _____(specialty)_____, you are invited to participate as a member of the System Safety Audit Team that will conduct a System Safety Audit of the above reference project on or about _____(date)_____ at _____(location)_____. A familiarization meeting will be held on _____(date)_____ at _____(time)_____ in room _____(number)_____.

The attached documents contain an outline of the agenda for the familiarization meeting (prior to the on-site visit) and indicates your primary area of expertise and responsibility. Your comments, however, are welcome in any areas of the systen under review for which you feel qualified to provide safety information. You can most effectively assist in the conduct of the System Safety Audit by adhering to the following precepts:

a. Review System Safety Procedure No._____: Establishing a System Safety Audit.

b. Study the attached inventory documents before arriving at the familiarization meeting. The inventory provides you with the information needed to discuss the safety aspects of the plan/system/equipment.

c. Notify the audit chairman or his designated representative immediately if, during your review of the inventory, you discover major discrepancies or oversights. Your prompt action can save the time of all team members during the on-site audit.

Figure C-1. Sample Audit Team Participation Request.

SYSTEM SAFETY AUDIT (SSA)

Audit No. _____
Contract No. _____
Audit Date _____

Project	Plant/System/Equipment	Location

TYPE OF AUDIT

- ☐ Preliminary
- ☐ Special
- ☐ Major

CONDUCTED BY

- ☐ Project Management
- ☐

AUDIT SCOPE OR PROJECT PHASE

- ☐ Exploratory Research
- ☐ Subsystem Development
- ☐ Pilot Plant
- ☐ Applications Experiment
- ☐ Structural
- ☐ QA, RA, Safety
- ☐ Electrical
- ☐ Chemical
- ☐ All Factors
- ☐ Equipment

LEVEL

- ☐ System
- ☐ Subsystem
- ☐ Equipment
- ☐ Component
- ☐ Plant

SYSTEM SAFETY AUDIT TEAM (SSAT) MEMBERSHIP

Area of Responsibility (1)	Name	Org. Code	Area of Responsibility (2)	Name	Org. Code
SSA Chairman			Human Factors		
Project Manager			Fabrication		
Mat'ls Engineer			Thermal		
Qual Assurance			Welding		
Process Performance			Environmental		
Consultants			Maintainability		
			Quality		
			Test/Demonstration		
			Subcontract		
			Support		
			Maintenance		

Notes: (1) Recommended for all SSA
(2) Should be included in SSA as applicable, particularly in a major SSA

Figure C-2. Sample System Safety Audit Agenda.

2) System Safety Audit File. An audit file composed of necessary reference material and other documents to be used by the audit team should be established and maintained. A typical file could include:

- System safety audit agenda
- Requirements for performance, reliability, quality, safety, etc., that are specified in the contract or letter
- System design (including justification and alternate designs)
- System engineering (input-output data)
- Complete technical description, specifications, drawings, and diagrams
- Part and component lists and application information (applied stresses, etc.)
- Project schedule, including milestones
- Operational, maintenance, and test plans
- Test data, analyses, (tolerance, stability, etc.) and technical information (manuals, reports, etc.)
- Data on process development unit, pilot or demonstration plants, systems, or equipment (including photographs of existing systems, subsystems)
- Know design deficiencies and other problem areas
- Changes to correct deficiencies
- Description of operator's duties
- Startup and shutdown (including emergency) procedures
- Physical and operational environments
- Storage transportation plans and requirements
- Training programs for operational and maintenance personnel
- Previous safety hazard analysis and failure mode and effects analysis

3) System Safety Audit Inventory. The audit team members should be provided a four-part audit inventory which includes technical documents, specifications, safety requirements, and other pertinent information. This audit inventory should be assembled and distributed in sufficient time to permit adequate documentation review prior to the familiarization meeting. The four-part inventory consists of:

Part I. Configuration Documentation - A listing of all pertinent descriptive material that is contained in the audit file

Part II. Design Requirements - a) A quantitative description of each environmental and functional design requirements, b) a performance estimation based on reasonable engineering judgments, and c) an identification of possible problem areas

Part III. Process Description - A detailed physical, functional, and fabrication description of the system design and safety, plus a summary of energy requirements and losses

Part IV. Evaluation - A discussion of performance versus safety requirements

See Figure C-3 for a sample inventory format.

e. Familiarization Meeting. A familiarization meeting should be planned and convened to acquaint team members with the project to be audited and to intitiate documentation required for the audit. Typical activities include technical presentation of:

- Project design (including concept considerations)
- Orientation to other units of the system
- Approaches to design and performance problems
- Other aspects of the project needed by the audit team to perform a valid audit
- Discussion of the supporting systems or equipment characteristics, for example, safety reliability, quality, materials
- Discussion and documentation of probable safety deficiencies for each category of the presentation and the audit inventory
- Review and summarization of the recommendations

5250-3 Vol. 5

SYSTEM SAFETY AUDIT INVENTORY
PART I

CONFIGURATION DOCUMENTATION

Audit No _____
Project _____
Plat/Sys/Equip _____
Contract No _____
Page No _____

Subject: CONFIGURATION DOCUMENTATION WHICH DEFINES AND SUPPORTS THE DESIGN

Supply the identification and dates of the applicable documents listed below, and list additional documents as required. Indicate by an asterisk (*) those items which have a direct bearing on the System Safety Audit (SSA) and attach copies to this inventory if not readily available to the System Safety Audit Team (SSAT) members.

SPECIFICATIONS, REQUIREMENTS, DESIGN OBJECTIVES

Contractor's Spec _____
Functional Reqmnts _____
Plant/Equip Reqmnts _____
System Design Obj _____
Item Design Obj _____
Support Design Obj _____
Power Subsystem Design Obj _____
Human Factor Reqmnts _____
_____

Plant/Equip Spec _____
Fabrication Spec _____
Test Spec _____
Subsystem Test Spec _____
Equip Test Spec _____
Subassembly Test Spec _____
Env. Test Spec _____
_____
_____

DESIGN DRAWINGS, DIAGRAMS, DATA

Master Index/List _____
Drawing List _____
Assembly Diag _____
Subassembly Diag _____
Materials List _____
Schematic Diag _____

Power Diag _____
Elect/Pwr Load Data _____
Block Diag _____
Functional Diag _____
_____
_____

ANALYSIS DOCUMENTS

Performance _____
Tolerance/Error _____
Reliability/Stress _____
Structure _____
Effectiveness _____
Capacity _____

Maintainability _____
Safety _____
Hazards _____
FMEA _____
Alternate Design _____
_____

For additional information contact _____ at _____

_____

Figure C-3. Sample System Safety Audit Inventory.

57

5250-3 Vol. 5

SYSTEM SAFETY AUDIT INVENTORY
PART 2

DESIGN REQUIREMENTS

Audit No_____
Project_____
Plant/Sys/Equip_____
Contract No_____
Page No_____

Subject: DE IGN REQUIREMENTS

List quantitative design requirements and the status of each (F-Firm; T-Tentative; U-Unknown) and the extent to which they have been achieved (i.e., estimated performance) based upon reasonable engineering judgement. Use item numbers from the list below. Comment on difficult or unusual problem areas.

ENVIRONMENTAL REQUIREMENTS TO BE CONSIDERED INCLUDE:

1. Temperature Range	6. Corrosion	11. _____
2. Material Temperature	7. Humidity	12. _____
3. Vibration	8. _____	13. _____
4. Shock	9. _____	14. _____
5. Pressure	10. _____	15. _____

FUNCTIONAL REQUIREMENTS TO BE CONSIDERED INCLUDE:

16. Plant Input	31. Parameter Distribution
17. Plant Output	32. Reliability
18. Volume	33. Quality
19. Weight	34. Maintainability
20. Cost	35. Human Factors
21. Stability	36. _____
22. Feedback	37. _____
23. Power Required	38. _____
24. Efficiency	39. _____
25. Cooling Limits	40. _____
26. Life	41. _____
27. Tolerance Limits	42. _____
28. Safety Factors	43. _____
29. Hazards	44. _____
30. Stress Distribution	45. _____

Figure C-3 (Cont 1). Sample System Safety Audit Inventory.

51

Item No	Quantitative Requirements Describe in Detail	F,T,U	Estimated Performance	Comments, Problem Areas

Figure C-3 (Cont 2). Sample System Safety Audit Inventory.

SYSTEM SAFETY AUDIT INVENTORY
PART 3

PROCESS DESCRIPTION

Audit No_____
Project_____
Plant/Sys/Equip_____
Contract No_____
Page No_____

Subject: PROCESS DESCRIPTION OF SYSTEM DESIGN AND SAFETY

The description of the system design and safety should include the following (as applicable):

1. APPLICATION/PHYSICAL DESCRIPTION (Reader Orientation)

State briefly the purpose and output of the project, the relation to similar projects, location, configuration, physical dimensions, and safety requirements (if any) imposed upon the project.

2. FUNCTIONAL DESCRIPTION (Detailed)

Describe the operation of the project in detail, block-by-block, part-by-part, for all modes of operation in every stage. Include block diagrams, schematics, sketches, curves, etc. to clarify the description, particularly inputs and outputs as to force, mass, heat, vibration, power factors, etc. Describe protection, fail-safe, and system safety features.

3. FABRICATION DESCRIPTION (Detailed)

Describe construction, volumetric efficiency, mounting, installation, structural soundness, thermal design, material applications, lubrication, mechanical and electrical clearances and tolerances, fabrication tolerances, welding quality, welding materials, etc. Include photographs, drawings and sketches to clarify the description.

4. ENERGY REQUIREMENTS AND LOSSES (Summary)

Describe, in tabular form, all forms and quantities of energy generated by the project, and provided and dissipated by it.

(Begin Description Here)

1. APPLICATION/PHYSICAL DESCRIPTION

Figure C-3 (Cont 3). Sample System Safety Audit Inventory.

SYSTEM SAFETY AUDIT INVENTORY
PART 4

EVALUATION

Audit No_____
Project_____
Plant/Sys/Equip_____
Contract No_____
Page No_____
Auditor_____

Subject: EVALUATION OF DESIGN AND SAFETY (Discussion of Performance versus Safety Requirements)

1. JUSTIFICATION OF DESIGN

Discuss why the project is designed like it is. Include sufficient calculations and data to permit assessment of the safety features versus the design. List and discuss any specification incompatibilities.

2. MATERIALS

Discuss all non-standard materials and processes used, provide sources of supply, status, procurement, and unusual environmental conditions which may be encountered.

3. RELIABILITY

Discuss what factors and features were included to assure failure-free operation over a specified period of time. State failure-free operating time estimate and show calculations.

4. TEST PROGRAMS

Discuss tests which verify safe performance of the project. Describe environmental test program and any specific facilities required. Describe start-up and shut-down test programs. Summarize test results to date, particularly data which indicates safety of the system.

5. FABRICATION CONSIDERATIONS

Identify critical fabrication areas that would cause functional problems which may result in a hazardous condition and a system safety problem, i.e., pressure drops, relief valves, etc. Discuss changes in fabrication which would improve system safety. Discuss inspection and quality programs and activities.

6. MAINTENANCE CONSIDERATIONS

Discuss the design from the viewpoints of maintainability, what controls are used to assure the quality of maintenance, and the resultant safety after a maintenance action.

Figure C-3 (Cont 4). Sample System Safety Audit Inventory.

SYSTEM SAFETY AUDIT INVENTORY
PART 4 – continued

EVALUATION

Audit No_____
Project_____
Plant/Sys/Equip_____
Contract No_____
Page No_____
Auditor_____

7. OPERATIONAL CONSIDERATIONS

Discuss the design from the viewpoint of providing operational safety for operating personnel, considering operating requirements, constraints, limitations, level of personnel, and simultaneous task requirements.

8. SUMMARY OF OTHER PROBLEMS

Summarize and discuss anticipated problems not adequately discussed elsewhere which may involve system safety or create a hazard resulting in unsafe operation or maintenance.

(Begin Evaluation Here)

1. JUSTIFICATION OF DESIGN

Figure C-3 (Cont 5). Sample System Safety Audit Inventory.

- Schedule the on-site verification and final audit report

- Develop the audit checklist

1) System Safety Audit Checklist. To ensure that all technical areas of photovoltaic systems or equipment are assessed for safety, an audit checklist should be developed. The checklist divides the project being audited into functional areas; for example, general design and fabrication, pressure vessels, switchgear, etc. Specific safety parameters are then listed for each of these areas. During the audit, the team member will examine each assigned area to determine whether the design is within the safety parameters and check one of the columns on the checklist: Acceptable, Non-Acceptable, Not Applicable. (See Figure C-4). The checklist need not be all-inclusive, but it should provide a guide to assist team members in reviewing the safety of design, construction, quality, reliability, maintainability, human factors, etc., of the project being audited.

f. Verification meeting

1) Scheduling. Provisions should be included in the procedure to ensure that appropriate personnel are notified for the on-site verification meeting, including the project manager and contractor personnel.

2) On-site Verification Meeting. The audit team should conduct on-site verification with project and contractor personnel in either a single meeting or a series of consecutive meetings. This depends on the complexity of the project and the type of audit. The agenda should include the following:

- A general discussion on the method of conducting the audit, the use of audit checklists, and the requirements for reporting audit findings

- A general site orientation, rules and regulations

- A discussion of the functional areas of the project

- A description of the on-site verification process

- A schedule for completion of on-site verification

- A schedule and place for the evaluation meeting

3) Verification Audit. Each team member should use the audit checklist previously developed to verify the safety of the area for which he is resposible, and then provide his findings and recommendations for corrective action. A sample recommended form is shown in Figure C-5.

SYSTEM SAFETY AUDIT

CHECKLIST_____

Item No.	Project: / Plant/Equipment: / Contract No.: Location / Audit No.: Date	Acceptable	Not Acceptable	Not Applicable
	GENERAL DESIGN AND FABRICATION (To Be Defined)			

Figure C-4. Sample System Safety Audit Checklist.

5250-3 UNC. 5

SAFETY AUDIT
RECOMMENDATIONS

Audit No _____
Project _____
Plant/Sys/Equip _____
Contract No _____
Page No _____
Auditor _____

TO: _____ Safety Audit Chairman

FROM: _____

Technical Specialty Area Audited: _____

Summarize your comments concerning the safety of the project, and list your recommendations. Submit this form to the Chairman at the close of the meeting. This form will become a part of the safety audit report.

NOTE: This is a suggested format, which may require additional space but paragraph headings and sequence should be retained.

COMMENTS

Summary of observations and findings:

RECOMMENDATIONS

I suggest that the following items be investigated or changed:

Figure C-5. Sample Recommendation for Corrective Action.

58

4) Audit Recording. Upon completion of the audit checklist and other on-site verification activities, each member of the audit team prepares a summary of his findings and makes recommendations in the area of his technical speciality. Specific recommendations about areas that should be changed or investigated should be cross-referenced to the checklist and/or other audit documents to support the recommdations. These summaries may then be used to prepare the audit report and substantiate the audit results.

5) Verification Closeout. Once the on-site verification is completed and checklists and recommendations are submitted, and before the team departs, a conference should be held with the appropriate project and contractor personnel to discuss the findings, recommendations, and corrective actions.

g. Debriefing and Evaluation. After on-site verification is complete, a meeting should be convened to discuss the team findings and recommendations. The agenda should include:

- Discussion of each functional safety area audited
- Assembly of the audit report
- Review of recommendations
- Overall assessment of project safety

h. Reporting. All information from the familiarization, verification, and evaluation meetings should be assembled and summaries prepared for inclusion in the final audit report. The final audit report can be organized as follows:

- Cover Sheets - Identifies the type of audit (preliminary, special, major); date of the report; approval signature(s); name of the project: the offfice or project publishing the report; signature of the chairman
- Executive Summary - Normally no longer than a single sheet (single spaced), that includes the highlights of the total audit process, including significant findings on safety and a summary of the recommendations
- Introduction - Contains project background information, previous safety audits and their outcomes, details of audit meetings, areas on which technical assessments and audits were conducted (materials, process, reliability, etc.), and the rationale used in establishing and conducting the audit. This section also includes summaries of the project, system, or equipment design, and project management highlights

- Technical Discussion - A description of the audit activities performed in each technical speciality area, audit findings, discussion of checklist items deficiencies observed, and recommendations to be considered

- Summary - A technical summary of the safety aspects of the project, including technical performance, project management, and all technical characteristics (reliability, quality, etc.) relating to system safety

- Findings and Recommendations - Comments on all team member recommendations and required corrective actions addressed to appropriate photovoltaics field center management should also be provided. See Figure C-6 for sample memorandum

i. Verification Followup. Before issuing the final report, the audit chairman may brief the appropriate field management personnel on the findings and recommendations in the report and also discuss any unresolved safety issues.

1) Project Action Report. A project action report is usually prepared by the field center project manager, and lists the acceptance or rejection of the report findings. The report identifies any corrective actions taken to resolve agreed-upon safety problems, and justification for rejecting any items. When initialed, the report becomes part of the final audit report. Followup reports are prepared periodically with copies sumitted to the audit file. A suggested report form is shown in Figure C-6.

2) Completed Final Report. Upon completion of the safety audit, the audit chairman will submit a completed final report to appropriate photovoltaics field center management personnel. Followup on incomplete action items and then notification of appropriate personnel when all system safety action items are completed is required.

5250-3 Vol. 5

SAFETY AUDIT

REPORT

To: _____

From: _____, Safety Audit Chairman

Subject: Transmittal of Final System Safety Audit Report.

1. A _____(type)_____ System Safety Audit was conducted on _____(project)_____ at _____(location)_____. The Project Manager is _____(name)_____. A pre-verification meeting was held on _____(date)_____ at _____(location)_____; an on-site verification meeting was held on _____(date)_____ at _____(location)_____; and a post-audit meeting was held on _____(date)_____ at _____(location)_____.

2. Members of the audit team are listed below together with their organization and area of specialty.

Name	Organization	Specialty

3. The final report in this audit is forwarded for your review and comment.

4. Should you have any questions regarding this audit or report please call _____(phone no.)_____.

5. Should you desire a formal presentation of the results of this audit or do discuss any of the recommendations, please contact _____(office)_____ at _____(phone no.)_____.

cc: TD&A PHOTOVOLTAIC LEAD CENTER
FIELD CENTER PROJECT MANAGER
Appropriate DOE management
Appropriate contractor(s)
File

Figure C-6. Sample Findings and Recommendations Memorandum.

61

System Safety Audit Project Action Report

Type of Audit_____ Date of Audit_____ Date of this Report_____

Project Name_____ Date of Initial Report_____

Project Manager_____ Organization_____

Findings/Recommendation	Action taken/status	Comment

Figure 7. Sample Project Action Report

APPENDIX D

SAMPLE SAFETY LIST

1. Provide black cloth or other suitable material to completely cover array to prevent power generation when maintenance is being performed on live electrical parts.

2. Any modules whose combined voltages exceeds 50 V should be provided with a disconnecting means to facilitate maintenance and troubleshooting procedures.

3. All systems should have lightning protection.

4. All systems should have a driven ground when system voltage exceeds 50 V.

5. All modules should have adequately-sized, factory-installed junction boxes as an integral part of the individual module.

6. Each module junction box should have insulated stand-off terminal blocks secured firmly to the junction box with metal screws or bolts.

7. All module junction boxes should have weathertight covers and weathertight cable entrances and exits.

8. Provision for battery disconnecting means is very important.

9. There should be provision for array disconnecting means, especially when array and distribution panel are not within sight of each other.

10. All loads on system should have adequate disconnecting means and branch circuit protection.

11. Adequate ventilation is imperative when large groups of batteries are in an enclosure.

12. Face mask, gloves, and acid neutralizing agent should be provided where groups of batteries are housed to protect personnel servicing the batteries.

13. All batteries should have flame arrestors.